Gigamon®

CrowdStrike + Gigamon Application Metadata Intelligence Deployment Guide

October, 2024

Pre-requisite:

Deploying Gigamon Application Metadata Exporter (AMX) VSN:

- Deploy a GigaVUE V series node (for AMX) with traffic acquisition method as Customer Orchestrated Source.
- And create a Monitoring Session (Rep1 (In) --->AMX --->Rep 2 (Out))

CrowdStrike:

- User should have their own http endpoint with API key, to which data has to be ingested.
- How to get create the http endpoint. → Configure the HTTP Event Connector with Datatype as JSON, and give your parser details.
- You will be able to get an endpoint along with the ingestion key, use this as part of the GIGAMON AMX config.

Configuration:

How to configure Gigamon Application Metadata Intelligence (AMI)

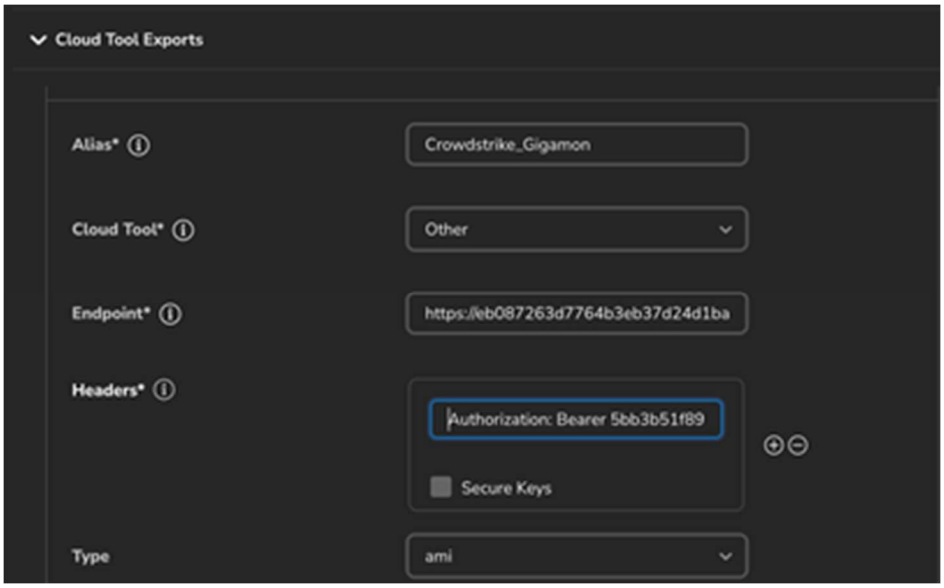
- Pls refer this public doc link: (Pls choose the release configuration guide corresponding to the running FM/Vseries)
- https://community.gigamon.com/gigamoncp/s/docs **- Doc Library**
- Below is the sample for 6.8 AMI
- Application Metadata Intelligence

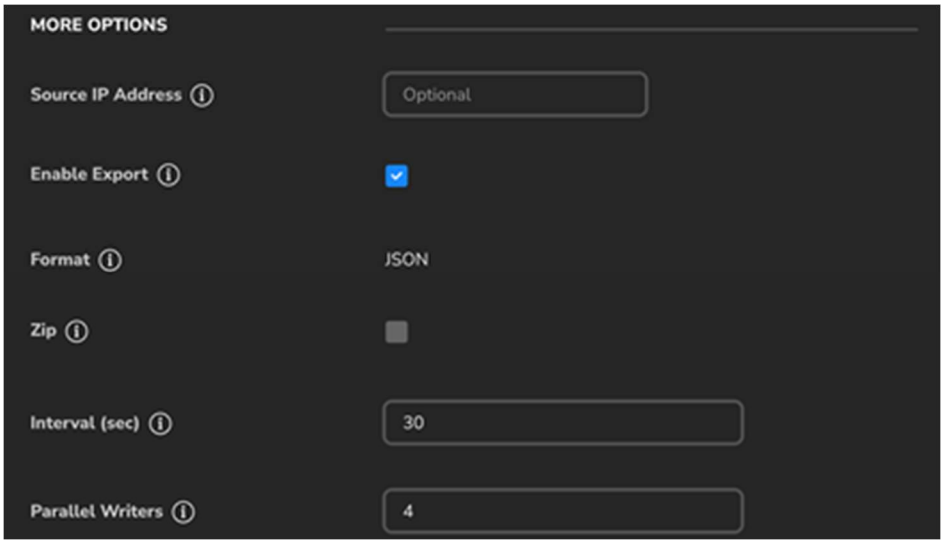
Configuring CrowdStrike Details in AMX:

- Please refer to the doc guide for details related to AMX configuration for 6.8: (Switch to corresponding release as required. As of 4th October 2024, 6.8 is the GA Release)

https://docs.gigamon.com/doclib68/Content/GV-Cloud-V-Series-Applications/AMX_intro.html?Highlight=AMX

- Edit the MS, Click on AMX and give details.
- Go to Cloud Tools Exports :
- Configure Alias as "CRWD or name as desired by the user"
- Cloud Tool as "Other"
- configure the Endpoint as per your HEC config
- Add a header to give the authorization key in this format "Authorization: Bearer 5bb3b51f89a346cf906"
- Type as "AMI"
- Enable Export
- Make sure you provide Label with "Key" as "event" and "value" as "Gigamon"
- Others with default values.
- Below is the snapshot:


Cloud Tool Exports
Alias*
Crowdstrike_Gigamon
Cloud Tool*
Other
Endpoint*
https://eb087263d7764b3eb37d24d1ba
Headers*
Authorization: Bearer 5bb3b51f89
Secure Keys
Type
ami

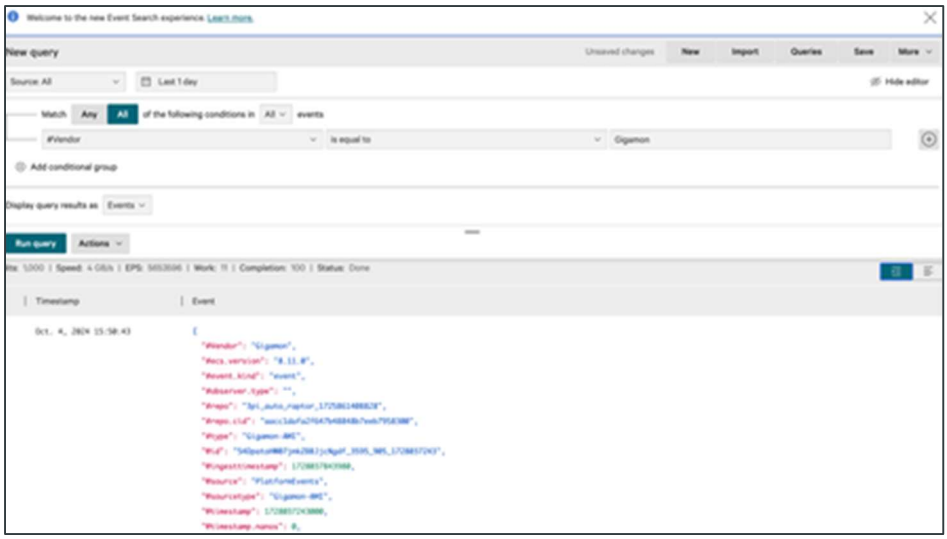

MORE OPTIONS
Source IP Address
Optional
Enable Export
Format
JSON
Zip
Interval (sec)
30
Parallel Writers
4


Export Retries
4
Max Entries
1000
Labels*
Key
event
Value
Gigamon

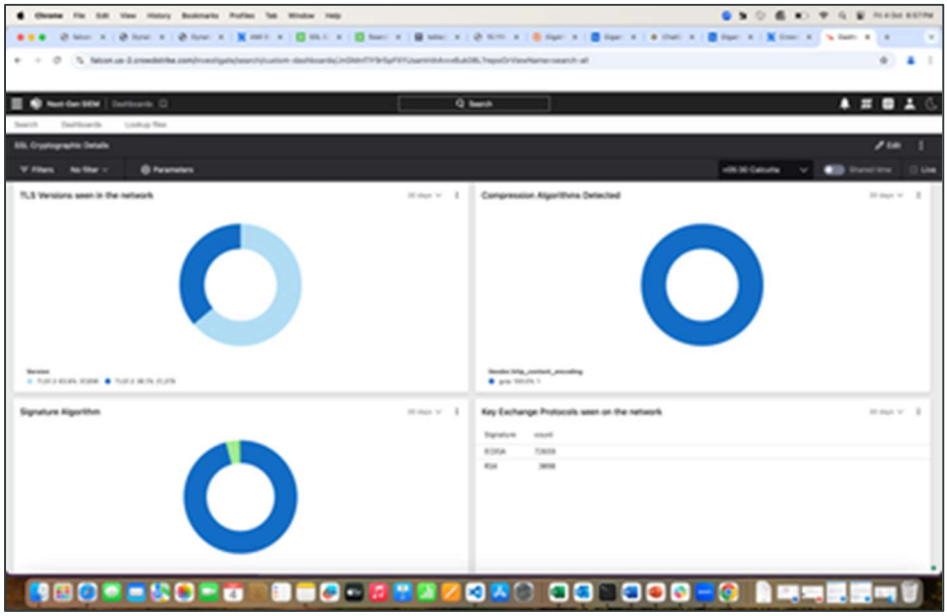
- Now click save and deploy the monitoring session.
- The configuration part is done, now you can test by sending traffic.

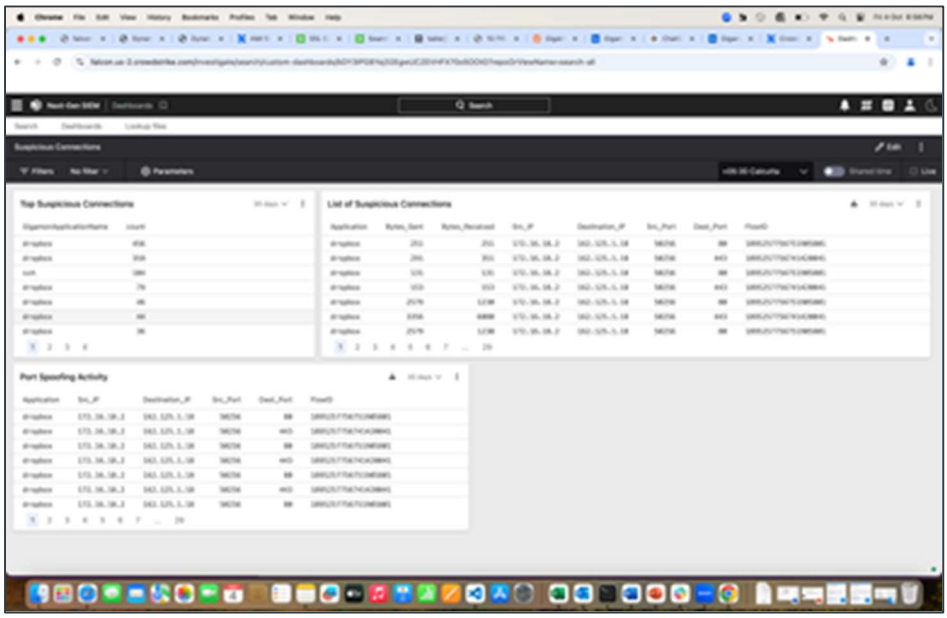
Configuring CrowdStrike to Ingest Json data:

- Login to crowd strike NGSIEM
- Go to Homepage --> NG SIEM → Event Search → Check for Vendor as Gigamon in the query, you will be able to see the below content if the ingestion is successful.



Below are the sample dashboards





Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com